# 证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2002 07 18

申　请　号：　02 1 26618.2

申请类别：　发明

发明创造名称：　一种防御网络传输控制协议同步报文泛滥攻击的方法

申　请　人：　华为技术有限公司

发明人或设计人：杨勇；滕新东；姜宏洲；李鸣雷；赵强；郑飞；杨建森；郭景泽；祈延

中华人民共和国
国家知识产权局局长　王景川

2002 年 12 月 9 日

# 权　　利　　要　　求　　书

1、一种防御网络传输控制协议同步报文泛滥攻击的方法，其特征在于该方法包括以下各步骤：

（1）防火墙接到来自客户机的连接请求，代理服务器向客户机返回同步应答报文，提示客户机暂时不传送有效数据；

（2）防火墙建立面向该连接请求的 相关信息记录，同时检验客户机连接请求的合法性，若防火墙没有接到客户机的确认应答报文，则该连接请求为非法，不进行处理，若接收到客户机的确认应答报文，则该连接请求为合法， 防火墙代理客户机向服务器发送连接请求；

（3） 防火墙接到来自服务器的同步应答报文，向服务器返回确认应答报文，同时防火墙代理服务器给客户机发窗口为非0的确认应答报文，启动客户机的数据传输；

（4）数据报文通过防火墙的代理在客户机与服务器之间转发，防火墙根据该连接的相关信息记录，进行报文的序列号变换。

2、如权利要求1所述的方法，其特征在于其中第（1）步的处理流程，包括以下步骤：

（1）防火墙收到客户机 同步请求报文，记录该报文的序号和窗口；

（2）防火墙产生一个序号作为源序号，构造窗口为 0的同步应答报文；

（3）防火墙将该同步应答报文发给客户机。

3、如权利要求1所述的方法，其特征在于其中第（2）步的处理流程，包括以下步骤：

（1）防火墙收到客户机对上述同步应答报文的确认应答报文后，记录该报文的序号和窗口；

（2）防火墙使用客户机发出连接请求时的序号和端口号，构造目的地址为服务器、源地址为客户机的同步报文，并将其发给服务器。

4、如权利要求1所述的方法，其特征在于其中第（3）步的处理流程，包括以下步骤：

（1）防火墙对来自服务器的同步应答报文进行序号检查，记录该报文的序号和窗口；

（2）防火墙构造目的地址为服务器、源地址为客户机的同步应答报文，并将其发给服务器；

（3）防火墙构造目的地址为客户机、源地址为服务器的窗口为非0的确认应答报文，并将其发给客户机。

5、如权利要求1所述的方法，其特征在于其中第（4）步的处理流程，包括以下步骤：

（1）防火墙对接收到的客户机的数据报文，使报文的源序号、窗口尺寸保持不变，使报文确认序号作相应的递增，然后发给服务器；

（2）防火墙对接收到的服务器的数据报文，使报文的确认序号、窗口尺寸保持不变，使报文的源序号作相应的递减，然后发给客户机。

# 说　　明　　书

## 一种防御网络传输控制协议同步报文泛滥攻击的方法

### 技术领域

本发明涉及一种防御网络传输控制协议同步报文泛滥攻击的方法，属于计算机网络安全技术领域。

### 技术背景

传输控制协议（Transmission Control Protocol，以下简称TCP）是因特网使用的三层传输协议之一，是许多网络应用的基础。传输控制协议同步报文泛滥攻击（Transmission Control Protocol Synchronous Package Flood Attack，以下简称TCP SYN Flood攻击）是网络中常见的一种拒绝服务攻击。该攻击实施简单，但破坏力极强，能使被攻击服务器资源耗尽，甚至操作系统崩溃，从而无法响应正常服务请求。

TCP SYN Flood攻击是在TCP建立连接的三次握手过程中进行的攻击，它的目标是耗尽被攻击主机资源，使其无法响应正常服务请求。假设一个客户机向服务器发送了TCP建立连接请求（TCP 同步报文）后突然死机或掉线，那么服务器在发出同步应答报文后就无法收到客户机的确认应答报文，即第三次握手无法完成，这种情况下服务器一般会重试（再次发送同步应答报文给客户机）。若等待一段时间后，仍未收到客户机的确认应答报文，则丢弃这个未完成的连接。正常情况下，只会出现少量的这种异常。但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源，当这种情况足够多时，最后的结果往往是服务器堆栈溢出崩溃。同时，由于服务器端忙于处理攻击者伪造的TCP连接请求，无法响应正常请求，此时从正常客户机的角度看来，服务器失去响应。这种情况就是TCP SYN Flood攻击。为防御TCP SYN Flood 攻击，被攻击的服务器自身可以采取一些有限的方法，但这些

方法针对不同的系统，只在特定情况下有效。实际网络中大都采用防火墙来防御TCP SYN Flood攻击。

目前在防火墙中防御TCP SYN Flood攻击常使用的方法是进行TCP连接监控，该方法的工作原理如图1所示，其工作过程如下：

1、防火墙接到来自客户机的连接请求（TCP 同步报文），将该连接请求转发至服务器；

2、服务器响应该连接请求，并将其返回给防火墙，防火墙将该同步应答报文转发至客户机；

3、防火墙向服务器发送确认应答报文；

4、这时，根据连接请求是否合法，可能有以下两种情况发生：

(a) 如果来自客户机的连接请求合法，防火墙将客户机的确认应答报文转发至服务器，服务器会忽略该确认应答报文，因为一个完整的TCP连接已经建立；

(b)如果来自客户机的连接请求非法（源IP地址非法），或没有在规定的时间内收到确认应答报文，防火墙向服务器发送复位报文，服务器拆除该连接。

上述方法可以在一定程度上防御TCP SYN Flood攻击，但有一个明显的缺点，即不论是否合法的连接请求都直接转发至服务端，待判断为非法连接时才采取措施拆除连接，因而TCP SYN Flood攻击还是影响到服务器，浪费了服务器端系统的资源。

发明内容

本发明的目的克服已有技术浪费服务端系统资源的缺点，提出一种防御网络传输控制协议同步报文泛滥攻击的方法，确保被保护服务器完全不受TCP SYN Flood攻击破坏。

本发明提出的防御网络传输控制协议同步报文泛滥攻击的方法，包括以下各步骤：

1、防火墙接到来自客户机的连接请求，代理服务器向客户机返回同步应答报文，提示客户机暂时不传送有效数据；

2、防火墙建立面向该连接请求的 相关信息记录，同时检验客户机连接请求的合法性，若防火墙没有接到客户机的确认应答报文，则该连接请求为非法，不进行处理，若接收到客户机的确认应答报文，则该连接请求为合法， 防火墙代理客户机向服务器发送连接请求；

3、 防火墙接到来自服务器的同步应答报文，向服务器返回确认应答报文，同时防火墙代理服务器给客户机发窗口为非0的确认应答报文，启动客户机的数据传输；

4、数据报文通过防火墙的代理在客户机与服务器之间转发，防火墙根据该连接的相关信息记录，进行报文的序列号变换。

上述第2步中的相关信息记录为：在后续处理过程中用于记录来自客户机或服务器的报文的序号、确认序号和窗口。

本发明的方法，在TCP报文传输过程中，防火墙拦截所有到达的连接请求，并代表服务器建立与客户机的连接，代表客户机建立与服务器的连接。如果两个连接都成功地建立，防火墙就会将两个连接进行中继，因此只有合法的TCP连接请求才会转发至服务端，不是待判断为非法连接时才采取措施拆除连接，避免浪费服务端系统资源。在监视模式下，防火墙被动地观察半开连接数，如果超过了所配置的阈值，防火墙也会关闭连接。防火墙有更严格的超时限制，以防止其自身的资源被TCP SYN Flood 攻击耗尽。

附图说明

图1是已有防御TCP SYN Flood攻击方法的工作原理图；

图2是本发明的工作原理图，其中的序号为状态编号；

图3是各会话状态对应的序号和窗口尺寸；

图4是防火墙接收到客户机TCP同步报文处理流程图；

图5是防火墙接收到客户机第一个确认应答报文处理流程图；

图6是防火墙接收到服务器端同步应答报文处理流程图；

图7是防火墙接收到数据报文处理流程图。

具体实施方式

本发明方法的工作原理如图2所示，首先防火墙接到来自客户机的连接请求（TCP 同步报文），并使用尺寸为0的窗口代理服务器向客户机返回一个同步应答报文，提示客户机暂时不传送有效数据。然后防火墙检验客户机连接请求的合法性，同时防火墙建立面向该连接请求的相关信息记录，该 相关信息记录为在后续处理过程中用于记录来自客户机或服务器的报文的序号、确认序号和窗口等等。若防火墙没有接到客户机的确认应答报文，则该连接请求为非法，不进行处理，若接收到客户机的确认应答报文，则该连接请求为合法， 防火墙代理客户机向服务器发送连接请求。 防火墙接到来自服务器的同步应答报文，同时向服务器返回确认应答报文，建立建立起防火墙与服务器之间的TCP连接， 防火墙代理服务器给客户机发窗口为非0的确认应答报文，启动客户机的数据传输。最后报文通过防火墙的代理在客户机与服务器之间转发，防火墙根据该连接的相关信息记录，进行报文的序列号变换。

为了更清楚地描述本发明方法的内容，首先对会话状态进行定义，本方法将连接发起端称为客户，对端称为服务器，它们通过防火墙的中继进行通信。客户发起连接，防火墙并不把TCP同步报文传递给服务器，而是自己伪装成服务器返回应答；客户确认后再以当初客户发起连接时的信息向服务器发起连接。当客户和服务器之间传输的数据报文通过防火墙时，防火墙只需对它们的序号进行调整就可以了。在这个过程中包含着若干会话状态，定义见表1，各会话状态对应的序号和窗口尺寸如图3所示。

表1：会话状态表

| 状态编号 | 名称 | 序号 / 确认序号 / 窗口 |
|---|---|---|
| 1 | 客户机发TCP同步报文 | S1 / 0 / W1 |
| 2 | 向客户机回同步应答报文 | S2 / S1+1 / 0 |
| 3 | 客户机发确认应答报文 | S1+1 / S2+1 / W2 |

| | | |
|---|---|---|
| 4 | 向服务器发TCP同步报文 | S1 / 0 / W1 |
| 5 | 收到服务器同步应答报文 | S3 / S1+1 / W3 |
| 6 | 向服务器回确认应答报文 | S1+1 / S3+1 / W2 |
| 7 | 向客户机发非0窗口确认应答报文 | S2+1/S1+1/W3 |
| 8 | 连接建立后向服务器发数据包 | Sx / Sy+(S3-S2) / W4 |
| | 连接建立后向客户发数据包 | Sx-(S3-S2) / Sy/ W5 |

上述表1与图3、图4、图5、图6、图7中使用的符号说明：

S代表序号，W代表窗口；

S或W与后跟的数字的组合代表特定的序号或窗口；

Sx和Sy在状态8中出现，代表一个不特定的序号（两者不相等）。

本发明的方法，包括按时间顺序进行的以下四个处理流程：

(1) 防火墙接收到客户机TCP同步报文后的处理流程，即图2和表1中的状态1和2；

(2) 防火墙接收到客户机第一个确认应答报文后的处理流程，即图2和表1中的状态3和4；

(3) 防火墙接收到服务器端同步应答报文后的处理流程，即图2和表1中的状态5、6和7；

(4) 防火墙接收到数据报文后的处理流程，即图2和表1中的状态8。

上述第一步的防火墙接收到客户机TCP同步报文处理流程如图4所示，防火墙收到客户机TCP同步报文，记录其序号和窗口，在后面流程中完成客户发起的连接建立过程以后向服务器发起连接时要用到。随后防火墙产生一个序号作为源序号，窗口设为 0（要求客户机暂时不要发送数据）构造同步应答报文，源地址不能用防火墙地址，必须用服务器地址。防火墙将该同步应答报文发给客户机。

上述第二步防火墙接收到客户机第一个确认应答报文处理流程如图5所示，此时防火墙正在等待客户机对防火墙发送的同步应答报文的确认应答报文。防火墙收到客户机的确认应答报文后，要进行序号检查，记录窗口W2，在作为客户机向服务器发起连接的流程中会用到。此时客户机与防火墙的连接已经完全建立，防火墙要与服务器进行连接并根据从服务

器得到的信息向客户机发确认。防火墙使用前面流程记录的客户机发起连接时的序号和端口，目的地址设为服务器，源地址设为客户机，构造TCP同步报文发给服务器。

上述第三步防火墙接收到服务器端同步应答报文处理流程如图6所示，防火墙收到服务器的同步应答报文，进行序号检查，记录来包的序号和窗口。然后，防火墙构造目的地址为服务器、源地址为客户机的同步应答报文，并将其发给服务器；构造目的地址为客户机、源地址为服务器的窗口为非0的确认应答报文，并将其发给客户机。此时防火墙认为客户机和服务器的连接已经完全建立。

上述第四步防火墙接收到数据报文处理流程如图7所示，在客户机与防火墙之间和防火墙与服务器之间的两个连接建立后，防火墙对客户机和服务器之间的数据报文只需进行序号调整，其它域保持不变。防火墙按以下方法调整数据报文序号（其中S2、S3是在流程1和3中记录的）：对接收到的客户机的数据报文，报文源序号、窗口保持不变，报文确认序号增加（S3－S2），然后发给服务器；对接收到的服务器的数据报文，报文确认序号、窗口保持不变，报文源序号减少（S3－S2），然后发给客户机。

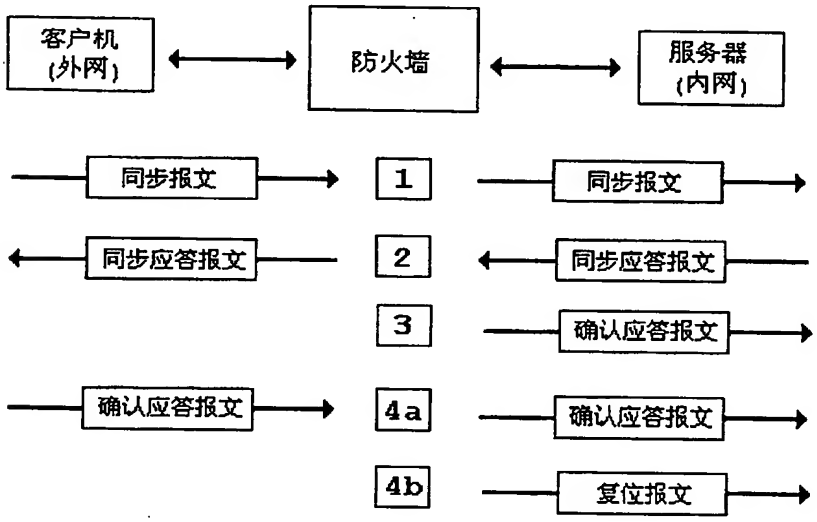
客户机
(外网)
防火墙
服务器
(内网)
同步报文
1
同步报文
同步应答报文
2
同步应答报文
3
确认应答报文
确认应答报文
4a
确认应答报文
4b
复位报文

图1

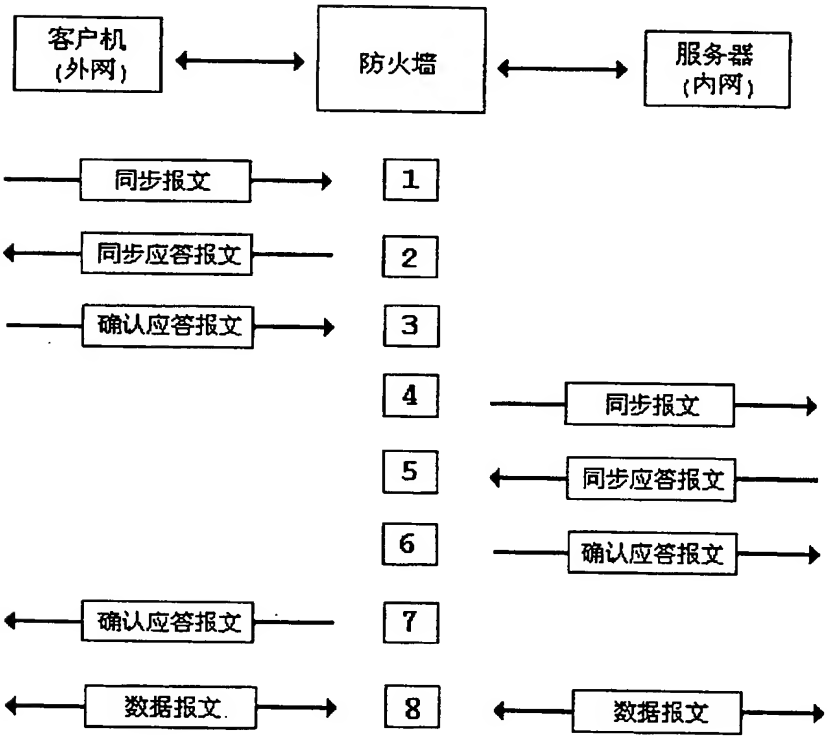
客户机
(外网)
防火墙
服务器
(内网)
同步报文
1
同步应答报文
2
确认应答报文
3
4
同步报文
5
同步应答报文
6
确认应答报文
确认应答报文
7
数据报文
8
数据报文

图2

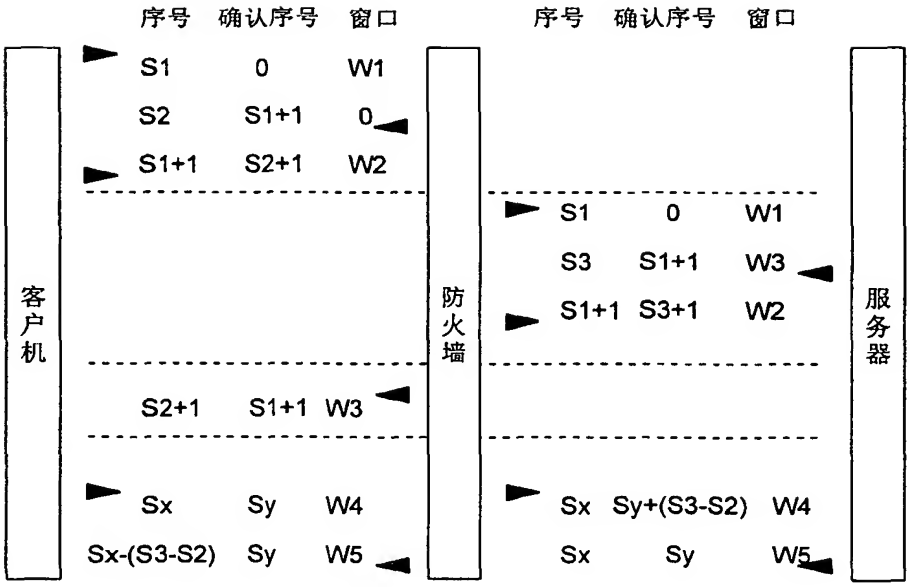
序号 确认序号 窗口
S1 0 W1
S2 S1+1 0
S1+1 S2+1 W2
S2+1 S1+1 W3
Sx Sy W4
Sx-(S3-S2) Sy W5
客户机
防火墙
序号 确认序号 窗口
S1 0 W1
S3 S1+1 W3
S1+1 S3+1 W2
Sx Sy+(S3-S2) W4
Sx Sy W5
服务器

图3

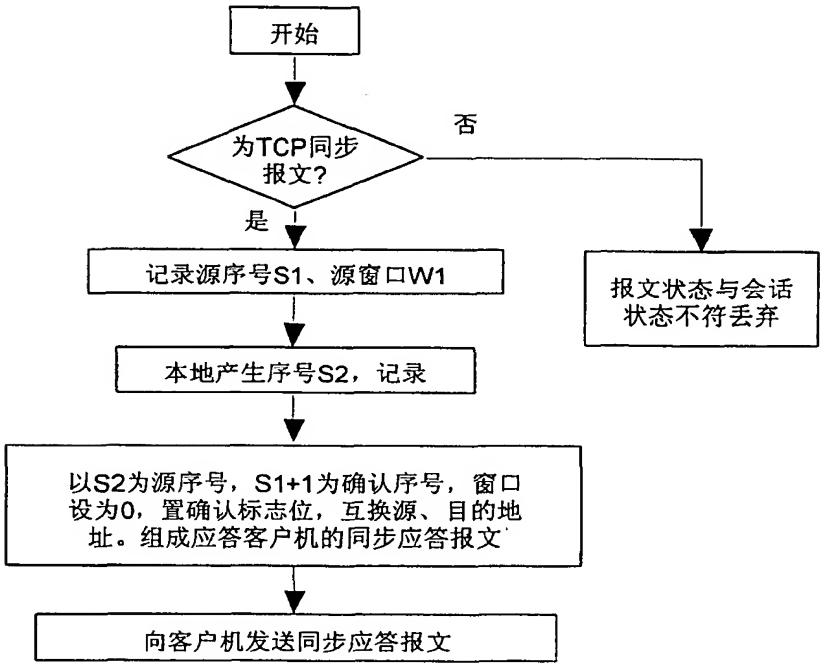
开始
为TCP同步报文?
否
是
记录源序号S1、源窗口W1
报文状态与会话状态不符丢弃
本地产生序号S2，记录
以S2为源序号，S1+1为确认序号，窗口设为0，置确认标志位，互换源、目的地址。组成应答客户机的同步应答报文
向客户机发送同步应答报文

图4

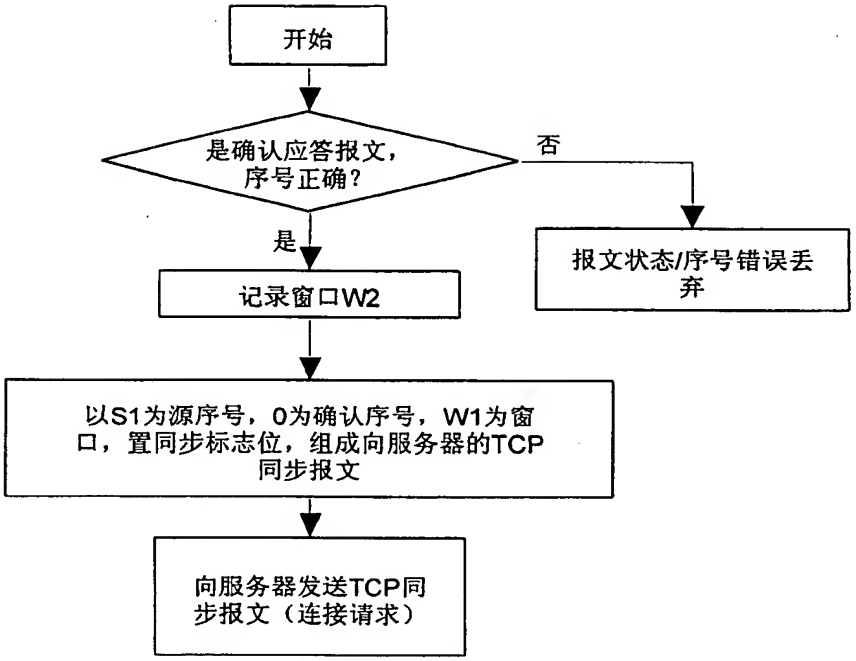
开始
是确认应答报文，序号正确？
否
是
报文状态/序号错误丢弃
记录窗口W2
以S1为源序号，0为确认序号，W1为窗口，置同步标志位，组成向服务器的TCP同步报文
向服务器发送TCP同步报文（连接请求）

图5

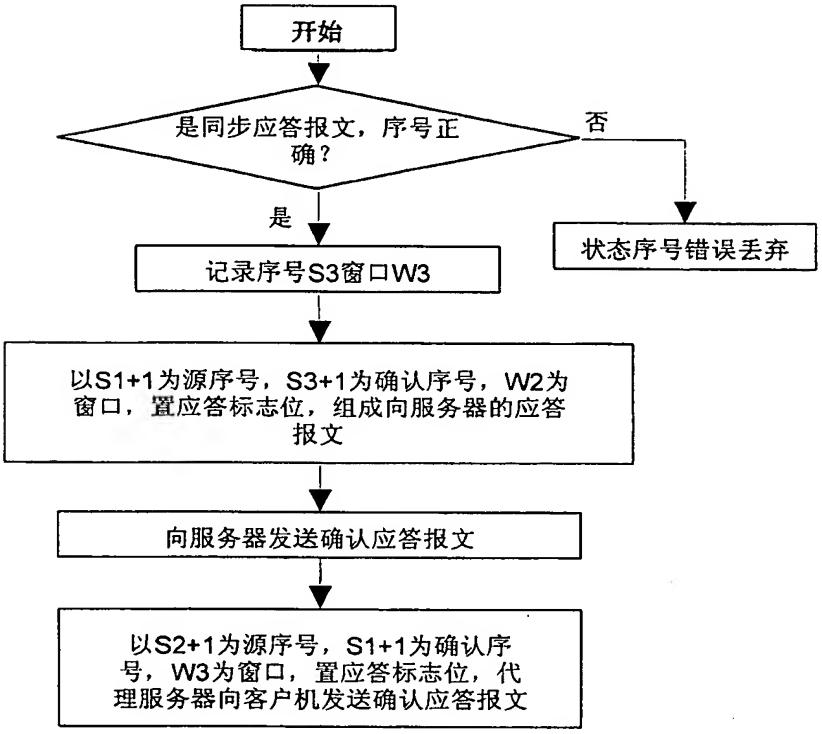
开始
是同步应答报文，序号正确？
否
是
状态序号错误丢弃
记录序号S3窗口W3
以S1+1为源序号，S3+1为确认序号，W2为窗口，置应答标志位，组成向服务器的应答报文
向服务器发送确认应答报文
以S2+1为源序号，S1+1为确认序号，W3为窗口，置应答标志位，代理服务器向客户机发送确认应答报文

图6

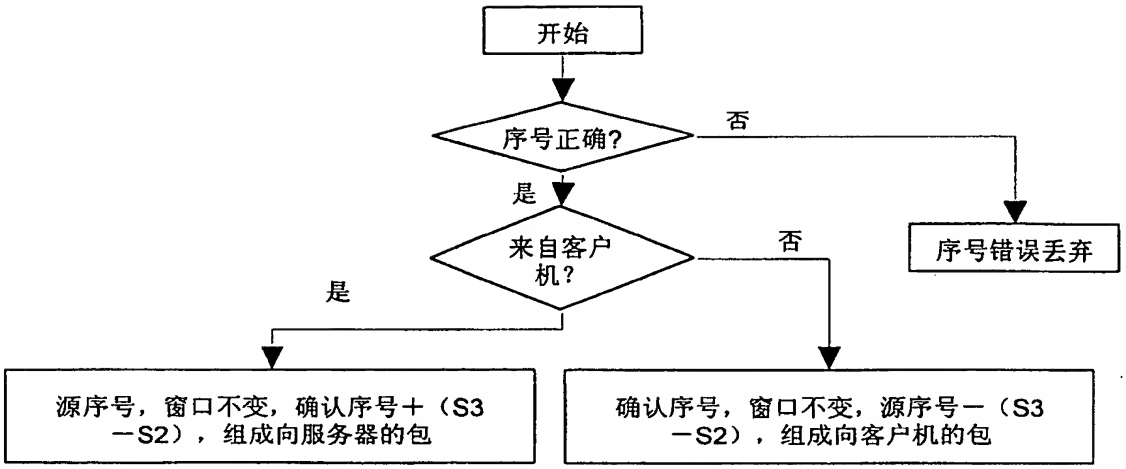
开始
序号正确?
否
序号错误丢弃
是
来自客户机?
否
是
源序号，窗口不变，确认序号＋（S3－S2），组成向服务器的包
确认序号，窗口不变，源序号－（S3－S2），组成向客户机的包

图7